REMARKS

The above amendments and following remarks are submitted under 37 C.F.R. 1.116 in response to the Final Official Action of the Examiner mailed July 2, 2002. Having addressed all objections and grounds of rejection, claims 1-20, being all the pending claims, are now deemed in condition for allowance. Entry of these amendment and reconsideration to that end is respectfully requested.

The Examiner has chosen to make the pending official action final, even though it is premature. It is premature, because it does not comport with MPEP 706.07(a) which states in part:

> Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's' amendment of the claims nor based on information submitted in an information disclosure statement filed during the period st forth in 37 CFR 1.87ith the fee set forth in 37 CFR 1.117(p). (emphasis added)

Since his previous rejection of claims 1-20, the Examiner has relied upon new prior art (i.e., article by Sabrina De Capitani di Vimercati) in rejecting all claims. He has further newly rejected claims 1-20 under both 35 U.S.C. 112, first and second paragraphs. Thus, it is indisputable that the pending official

action "introduces a new ground of rejection". Yet, the Examiner has prematurely made the present rejections final in defiance of MPEP 706.07(a). Nevertheless, even though the present official action has been made prematurely final, Applicants are obligated to respond on the merits by way of an amendment under 37 C.F.R. 1.116 to avoid abandonment of the subject application.

The Examiner has objected to the specification noting certain informalities at page 27, line 21, at page 28, line 2, and at page 33, line 23. The above amendments to the specification are deemed fully responsive to this ground of objection.

The Examiner has further objected to the specification alleging "inconsistencies between different sections of the specification". He states:

> In the Summary of the Invention, pages 7-9, a site-specific security profile is discussed, such that there is no need to transmit UserID/password information across a publicly accessible network. However, in connection with Figure 10, replacement pages 33-34, the Detailed Description of the Preferred Embodiments discusses the user's service request resulting in the execution of a command language script with associated security profile which requires the user to submit a UserID over the World Wide Web in order for the execution of the script to proceed.

The Examiner has apparently misunderstood Applicants' disclosure. At page 7, lines 11-13, Applicants state:

> This invention will provide a new SignOn capability which allows for site-specific data to be used to identify a user. The site-specific data is converted to a valid UserID/Password by a User Validation service implemented by a site.

As is clearly and specifically disclosed, the user terminal creates a "valid UserID/Password" during the user SignOn process which identifies the user terminal site utilized rather than by the actual user having a personal UserID/Password. It is this site-specific "valid UserID/Password" which is transferred to the server as stated at page 34, lines 10-13:

> However, if a security profile has been identified for the service request, service handler 322 requests the user to provide a user-id via path 330, Cool ICE object 322, and world wide web path 312. Service handler 332 awaits a response via world wide web path 308, Cool ICE object 322, and path 326.

This process is summarized at page 7, lines 16-18:

> This unique User Validation feature provides the capability for the browser to send information, which is then translated into a UserID/Password on the Cool ICE Web Application server. This bypasses the need to send a UserID/Password from browser to server, which enhances security.

It is this feature which is consistently disclosed and claimed throughout the subject application.

The Examiner continues stating:

> The examiner has failed to locate a disclosure of site-specific security profile anywhere in the Detailed Description of the Preferred Embodiments.

Whereas this statement may be true on its face, it does not diminish the fact that Figs. 13-14 are specifically directed to "site-specific security profile" generation and use. Page 11, lines 2-3, states:

> **Fig. 13** is a diagram showing the creation of a site security profile; and
> **Fig. 14** is a listing of the messages utilized in creating the site security profile.

Because these drawings are quite "verbal" and are deemed essentially self-explanatory, the accompanying descriptions in the specification are somewhat brief.

The Examiner has rejected claims 1-20 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. This ground of rejection is respectfully traversed. The Examiner states:

> The claim limitations of the independent claims regarding the use of a physical site specific security profile in permitting access to a database without requiring the transfer of a user identifier via a publicly accessible digital data communications network (claims 1, 6, 11 and 16) are discussed in the Summary of the Invention, pages 7-9. However, the details of the use of the physical site specific security profile is not disclosed in the Detailed Description of the Preferred Embodiments, and in fact the section of the Detailed Description concerning the operation of security profiles discloses a mechanism whereby a user submits a service request which results in the execution of a command language script with associated security profile which requires the user to submit a UserId over the World Wide Web in order for the execution of the script to proceed. This disclose is

> inconsistent with the claim language. The lack of a detailed disclosure of the claimed invention renders the invention non-enabled.

As explained above, the Examiner is incorrect in his assessment. The user signs on with his/her personal UserID/Password. From site-specific information, the user terminal creates a "valid UserID/Password" which is peculiar to the user terminal site, rather than the individual user. The process of "creation of a site-specific security profile" is shown in Fig. 13. The messages associated with the creation process are shown in Fig. 14.

However, it is acknowledged that the specification does not refer to "physical" site or location. As a result, Applicants have amended the claims to remove this term. The rejection of claims 1, 6, 11, and 16 is respectfully traversed concerning the claims as amended.

The Examiner has further rejected claims 2-5, 7-10, 12-15, and 17-20, stating:

> Claims 2-5, 7-10, 12-15 and 17-20 are also rejected as being non-enabled, inheriting the deficiencies of their parent independent claims, and further more because other claimed details, such as the "special field" of claims 3, 7, 13 and 17, and the mechanism for the generation of the physical site specific security profile by the database management system (claims 3 and 6), are not disclosed in the specification.

This ground of rejection is respectfully traversed as based upon clearly erroneous findings of fact. Page 8, lines 4-7, states:

> In the preferred embodiment of the present invention, site specific security profiles are implemented using a secret field, which identifies the user terminal site. This identifier is utilized by the Cool ICE system to define the appropriate level of site security for the transferring user terminal.

For a more detailed description, the Examiner's attention is directed to the disclosure of Message #2 on Fig. 14. Regarding "the mechanism for the generation of the physical site specific security profile", the Examiner is directed to Fig. 13. The rejections under 35 U.S.C. 112, first paragraph, are respectfully traversed.

Claims 1-20 have been rejected under 35 U.S.C. 112, second paragraph, as being indefinite. This rejection is respectfully traversed for the reasons provided above.

In paragraph 9 of his final office action, the Examiner misdefines the invention. As a matter of law, the invention is defined by the claims.

The Examiner has rejected claims 1-4, 6-8, 11-14, and 16-18 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison") in view of U.S. Patent 6,237,023, issued to Yoshimoto (hereinafter referred to as "Yoshimoto") further in view of the

article, "Access Control in Federated Systems", by De Capitani di Vimercate et al (hereinafter referred to as "di Vimercati"). This ground of rejection is respectfully traversed.

As explained above, Applicants' invention as disclosed and claimed enables a user to identify himself/herself to the user terminal. In response thereto, the user terminal creates a site-specific UserID/Password for transfer to the server in association with a service request requiring access to secure data. Thus, the user can access the secure data based upon the site-specific UserID/Password without the need to transfer the user's personal UserID/Password to the server.

Even though the Examiner alleges an unwieldly combination of three disparate references, unlike Applicants' claimed invention, each of them requires transfer of the user's personal identification to the server. At Fig. 4A, element 111, Garrison requires the user to supply his/her personal password. Furthermore, Garrison states at column 10, lines 44-48:

> After receiving the new encryption key from the server 17a, the client 14 encrypts the user's password and log name with the new encryption key and transmits the password and log name to the server 17a, as shown by block 111 in FIG. 4A.

As admitted by the Examiner, Garrison has no site-specific security profile.

Similarly, Yoshimoto requires transfer of the user identifier to the server. The first sentence fragment of the Abstract states:

> When a server receives a service request from a client, identifiers of a terminal and of a suer are acquired from the service request and authority with respect to the service request is uniquely decided from the terminal and user identifiers acquired.

Further evidence of the need to transfer the User ID in Yoshimoto can be found at Fig. 2, element S202; Fig. 3, element S302; Fig. 4, element S401; and Fig. 5, element S501. Yoshimoto simply requires the user identifier to provide access to secure data.

Having admitted that neither Garrison nor Yoshimoto teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network, the Examiner has alleged the combination of yet another reference, di Vimercati. The new reference states at paragraph 2.1:

> A good user's authentication is a <u>prerequisite</u> for a correct access control. The identity of a user determines the groups to which the user belongs, the roles he can play (if applicable), and ultimately the privileges he is allowed to exercise. Even in mandatory systems, where clearances are used to access controls instead of identifiers, the user's identity is <u>needed</u> to determine the security level with which the user can connect to the system. In any case therefore, on a user's identity depends whether his requests to access the data will be allowed or denied. (Emphasis added)

Though di Vimercati is difficult to understand, it is apparent that transfer of the user identification is the principle element of the security process. This theme is repeated over and again. At paragraph 3.2, the reference states:

> To access a federation, a user must explicitly open a working session by connecting to the federation site. Connection requires identification of the user and corresponding authentication of his identity by the federation. (Emphasis added)

Thus, it is not readily understandable how the Examiner can make the clearly erroneous finding:

> De Capitani di Vimercati et al., however, teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

Quite apart from di Vimercati saying nothing of transferring anything over "said user identifier via said publicly accessible digital data communication network", just like Garrison and Yoshimoto, di Vimercati considers that "the user's identity is needed to determine the security level". For the Examiner to argue differently is to deny the clear teachings of the references.

In rejecting claim 2, the Examiner clearly erroneously states:

> Regarding claim 2, Garrison additionally teaches an improvement wherein said security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

The Examiner has admitted that Garrison does not teach an apparatus wherein the security profile is site-specific. Therefore, it is clearly erroneous to state that Garrison teaches "wherein said security profile is generated by said data management system. The rejection of claim 2 is respectfully traversed as based upon clearly erroneous findings of fact.

In rejecting claims 3, 8, 12-13, and 18, the Examiner clearly erroneously states:

> Regarding claims 3, 8, 12, 13 and 18, Garrison additionally teaches an improvement, method and apparatus further comprising a special field responsively coupled to a service requests whereby said database management system receives said special field and <u>generates said security profile corresponding to said site</u> and to said special field (see discussion of predefined password at col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37). (emphasis added)

Having admitted that Garrison does not have a "security profile corresponding to said site", it is baffling to see that the Examiner can find Garrison to contain these limitations.

In rejecting claims 5, 9, 10, 15, 19, and 20, the Examiner states:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER is extremely versatile and is considered one of the best fourth generation programs, and furthermore since it contains, in addition to a database management system, a word processor, office automation program including electronic mail, and color graphics routines (see King, first paragraph).

This statement is deemed clearly erroneous. The specification states at page 3, line 21, through page 4, line 6, states:

> However, with the MAPPER system, as well as with similar proprietary data base management systems, the user must interface with the data base using a terminal coupled directly to the proprietary system and must access and manipulate the data using the MAPPER command language of MAPPER. Ordinarily, that means that the user must either be co-located with the hardware which hosts the data base management system or must be coupled to that hardware through dedicated data links. Furthermore, the user usually needs to be schooled in the command language of MAPPER (or other proprietary data base management system) to be capable of generating MAPPER Runs.

These specific characteristics of MAPPER are deemed so inconsistent with the goals of Garrison, Yoshomoto, and di Vimercati, one or ordinary skill in the art would not look to make the alleged combination.

The rejection of claims 5, 9, 10, 15, 19, and 20 is respectfully traversed.

Having thus responded to each objection and ground of rejection, Applicants respectfully request entry of this amendment and allowance of claims 1-20, being the only pending claims.

Respectfully submitted,

Paul S. Germscheid, et al

By their attorney,

Date August 29, 2003

John L. Rooney
Reg. No. 28,898
Suite 401
Broadway Place East
3433 Broadway Street N.E.
Minneapolis, Minnesota
55413
(612) 331-1464